## DETAILED ACTION

1.      It is hereby acknowledged that the following papers have been received and placed of

record in the file: Amendment date 06/06/2011

2.      Claims 1, 12, 14, 16-17, 27-28, 39, 41, 43-48, 51-57 and 65 are presented for

examination.

3.      The rejections are respectfully maintained and reproduced infra for applicant's

convenience.


### *Response to Arguments*

4.      Applicant's arguments filed 06/06/2011 have been fully considered but they are not

persuasive.

5.      Applicant argues the following limitation(s):

•       Applicant argues, stated in the remark on page 13, "Robertson does not use a

public key to identify a computer." On the contrary, Robertson teaches unique identifier name

for the each IPSAP base server and server return IP addresses of the destination IPSAP based

server and public "Each IPSAP base server is given a unique identifier name (net-id) and Pretty

Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange

Formats) to identify … and then returning the IP addresses of the destination IPSAP based server

the PGP public key for the requested IPSAP base server" (see Robertson: ¶[0005]). The net-id

allows the user to identify the IP network being used at any given time (see Robertson: ¶[0007])

such as net-id is used to address server, and limits PGP key to their traditional authentication and

encryption functions. Robertson further teaches the user to use the net-id make connection to

IPSAN via network B (see Robertson: ¶[0013]), where the user's authentication information use

to identify where the user's authentication record are stored. Furthermore, Robertson teaches

multiple IPSAP base servers (14) in the figure 1, where IPSAP central server <u>returning the IP</u>

<u>addresses of the destination IPSAP server and PGP public key server</u>. Since Robertson teaches

the net-id and PGP public key for identify the IPSAN base servers, it clearly teaches the

limitation of use a public key to identify a server computer and the public key identifies a

plurality of server computers having different network addresses. Claims 12, 14, 16, 17, 27-28,

39, 41, 43 and 65 that depend on own corresponding independent claims are also not persuasive

based on the reasons above.

&bull;    Applicant argues, stated in the remark on pages 15 and 17, Kumar does not

discloses "searching an authentication record for the address of the server computer" in claims

44 and 54. On the contrary, Kumar teaches DNS lookup in the server computer for relating to the

requested URL is selected when URL not found in the local memory "Upon initiating a DNS

lookup, DNS searches and collects addresses relating to the requested URL host name" (see col.5

lines 38-40). Kumar further teaches searching URL host name in the memory for address of the

server at step 402, perform transfer step 410 when URL is found  either from memory or

replication server (see Kumar: Fig.4). In addition, Robertson further teaches the user 10 use the

net-id make connection to IPSAN via network B (see Robertson: ¶[0013]), where the user's

authentication information use to identify where the user's authentication record are stored.

Based on the reasons above,  Kumar combination with Robertson taught the searching an

authentication record for the address of the server computer.

- Applicant argues, stated in the remark on page 16, Robertson does not teaches the backup search procedure including searching a configuration record of the client computer system for the network address of the server computer." On the contrary, Robertson teaches software on the user's computer also determines additional public information about the IP network and then acquires configuration information from the IPSAP central server and the local IPSAP base server" (see Robertson: ¶[0007]). Since the user computer acquires configuration information from the IPSAP central server and local IPSAP base server for communication to other IPSAP base server via network B, it clearly teaches backup search procedure including searching a configuration record of the client computer system for the network address of the server computer.

- Applicant argues, stated in the remark on page 18, "the combination of Gulko and Kumar fails to disclose public key" and backup search procedure determining whether the server computer is running on a CPU that is the same CPU in which the client computer is running in order to determine the network address of the server computer". With respect to the public key, applicants fails to disclose public key in body of the claim 55. As the invention as whole, Gulko directed to parallel process and Kumar directed to URL resolving, it would have been obvious to one of ordinary skill in the art at the time of invention to perform parallel URL resolving to reduce computation time and increase in result accuracy (see Gulko: ¶[0012]). Furthermore Gulko teaches whether the resource on the same processor by using inter process communication (IPC) "That resource can be the same or another processor resident on the machine that is executing application 60, or can be another machine connected via a network 4" (see Gulko:

¶[0137]; ¶[0151]). Based on the reasons above, Examiner strongly believes applicant's arguments

have been fully considered but they are not persuasive.


### Claim Rejections - 35 USC § 103

6.       The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

7.       Claims 1, 12, 14, 16, 17, 27-28, 39,  41, 43-44, 47-48, 51-54 and 65  are rejected under

35 U.S.C. 103(a) as being unpatentable over Kumar et al. (US 6,795,434) in view of Robertson

et al. (US 2003/0196107 A1).

8.       Regarding claim 1, Kumar teaches a method for a client computer to find a network

address of a password server computer having a public key, the method comprising:

        searching for a network address (Best replicated server see Kumar: col.2 line 23) of the

server computer using a backup search procedure if the address of the server computer cannot be

identified using a primary search procedure (Searching the server's addresses using the initiate

DNS lookup when the URL not found in the memory cache "The process proceeds to block 402

to examine whether the requested URL host name is in the local cache memory" see Kumar:

col.5 lines 26-45; Fig. 4 steps 402-408); and

        establishing a connection with the server computer using the network address

found (Once detect the most preferred server address and establish to the server "The address

listed on the top of the sorted preferred list is the most preferred server address, which points to

the most preferred server or the optimal site is addressed by the most preferred server address"

see Kumar: col.7 lines 48-56; Fig.4 Step 410),

wherein:

the backup search procedure searches for the server computer using the public key to

identify the server computer (DNS lookup as backup search procedure "If the requested URL

host name is not in the cache, the process proceeds from block 402 to block 404, where the

process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37).

Kumar does not explicitly to disclose the public key is an identifier of the server

computer and the public key identifies a plurality of server computers having different network

addresses.

However Robertson teaches the public key is an identifier of the server computer and the

public key identifies a plurality of server computers having different network addresses (unique

identifier name for the each IPSAP base server and server return IP addresses of the destination

IPSAP based server and public "Each IPSAP base server is given a unique identifier name (net-

id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP

Message Exchange Formats) to identify … and then returning the IP addresses of the destination

IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson:

¶[0005]) in order to provide a workable system for allowing a user to authenticated across

multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) the public key is an identifier of the

server computer and the public key identifies a plurality of server computers having different

network address as taught by Robertson in order to provide a workable system for allowing a

user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

9.      Regarding claim 12, the modified Kumar taught the method of claim 1 as described

hereinabove. Robertson further comprising authenticating the server computer after the

connection has been established (remote authentication the IPSAP base server when allowing

building trust relationship between server and client "Remote Authentication Dial In User

Service (RADIUS) authentication (IETF RFC 2138) is used to interface the IPSAP base server

with the existing authentication program" see Robertson: ¶[0005]).

10.     Regarding claim 14, the modified Kumar taught the method of claim 1 as described

hereinabove. Kumar further comprising the step of populating a local storage of the client

computer with a list of network addresses for server computers after the connection has been

established (update the list of the server network address "At block 854, the process sorts the

addresses into a preferred list of site addresses according to the responses and data types" see

Kumar: col.9 lines 14-21).

11.     Regarding claim 16, the modified Kumar taught the method of claim 1 as described

hereinabove. Kumar further teaches wherein the primary and backup search procedures are

performed in parallel (either can based on hit and miss ratio or DNS lookup "the comparing unit

506 issues a message of cache-miss to indicate that IP server addresses are not in the cache 522.

Both the message of cache-miss and the message of cache-hit, which could be configured to one

message, are sent to the selecting unit 510 and DNS lookup unit 508" see Kumar: col.6 lines 44-

47).

12.     Regarding claim 17, claim 17 is rejected for the same reason as claim 1 as set forth

hereinabove.

13.     Regarding claim 27, claim 27 is rejected for the same reason as claim 16 as set forth hereinabove.

14.     Regarding claim 28, claim 28 is rejected for the same reason as claim 1 as set forth hereinabove.

15.     Regarding claim 39, claim 39 is rejected for the same reason as claim 12 as set forth hereinabove.

16.     Regarding claim 41, claim 41 is rejected for the same reason as claim 14 as set forth hereinabove.

17.     Regarding claim 43, claim 43 is rejected for the same reason as claim 16 as set forth hereinabove.

18.     Regarding claim 44, Kumar teaches a method for a client computer to locate a network address of a server computer on a computer network, said server computer having a public key that is an identifier of the server computer, the method comprising:

        searching for the address of the server computer in a local system storage of the client computer (Searching the URL in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 27-28); and

        performing a backup search procedure if the address is not found in the local system storage (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37),

the backup search procedure being <u>selected from a group</u> of search procedures consisting of the following:

broadcasting a message over the network to identify the address of the server computer,

searching an authentication record for the address of the server computer (DNS lookup in the server computer for relating to the requested URL is selected when URL not found in the local memory "Upon initiating a DNS lookup, DNS searches and collects addresses relating to the requested URL host name" see col.5 lines 38-40),

using a loop back address,

using a inter process communication to determine whether the server computer is running on a same CPU as the client computer in order to determine the network address, and

searching a configuration record of the client computer for the address of the server computer; and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key identifies a plurality of server computers having different network addresses.

However Robertson teaches the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key

identifies a plurality of server computers having different network addresses (unique identifier

name for the each IPSAP base server and server return IP addresses of the destination IPSAP

based server and public key "Each IPSAP base server is given a unique identifier name (net-id)

and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message

Exchange Formats) to identify … and then returning the IP addresses of the destination IPSAP

based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]) in

order to provide a workable system for allowing a user to authenticated across multiple IP

networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) the one or more of said search

procedures searches for the server computer using the public key to identify the server computer,

and the public key identifies a plurality of server computers having different network addresses

as taught by Robertson in order to provide a workable system for allowing a user to authenticated

across multiple IP networks and road at will (see Robertson: ¶[0004]).

19.     Regarding claim 47, claim 47 is rejected for the same reason as claim 16 as set forth

hereinabove.

20.     Regarding claim 48, Kumar teaches a system for finding a network address, the system

comprising:

client means for:

searching for the network address (Best replicated server see Kumar: col.2 line 23) of the

server means by searching for the address of the server means in a local system storage of the

client means (Searching the server's addresses using the initiate DNS lookup when the URL not

found in the memory cache "The process proceeds to block 402 to examine whether the

requested URL host name is in the local cache memory" see Kumar: col.5 lines 26-45; Fig. 4

steps 402-408),

using a backup search procedure to identify the address of the server means if the address

is not found in the local system storage  (DNS lookup as backup search procedure "If the

requested URL host name is not in the cache, the process proceeds from block 402 to block 404,

where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5

lines 34-37), and

establishing a connection with the server means using the network address found (Once

detect the most preferred server address and establish to the server "The address listed on the top

of the sorted preferred list is the most preferred server address, which points to the most

preferred server or the optimal site is addressed by the most preferred server address" see

Kumar: col.7 lines 48-56; Fig.4 Step 410),

wherein the client means is configured to search for the network address as the backup

search, the backup procedure being selected from a group of search procedures consisting of the

following:

broadcast a message over the network to find the address of the server means,

search an authentication record for the address of the server means (DNS lookup in the

server computer for relating to the requested URL is selected when URL not found in the local

memory "Upon initiating a DNS lookup, DNS searches and collects addresses relating to the

requested URL host name" see col.5 lines 38-40),

use a loop back address,

use a inter process communication to determine whether the server means is running on a

CPU that is the same CPU on which the client is running means in order to determine the

network address, and

search a configuration record of the client means for the address of the server means.

Kumar does not explicitly to disclose the server means having a network address and a

public key, the public key being an identifier of the server means; one or more of said search

procedures searches for the server means using the public key to identify the server means, and

the public key identifies a plurality of server computers having different network addresses.

However Robertson teaches the server means having a network address and a public key,

the public key being an identifier of the server means; one or more of said search procedures

searches for the server means using the public key to identify the server means, and the public

key identifies a plurality of server computers having different network addresses (unique

identifier name for the each IPSAP base server and server return IP addresses of the destination

IPSAP based server and public key "Each IPSAP base server is given a unique identifier name

(net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP

Message Exchange Formats) to identify … and then returning the IP addresses of the destination

IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson:

¶[0005]) in order to provide a workable system for allowing a user to authenticated across

multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) server means having a network address

and a public key, the public key being an identifier of the server means; one or more of said

search procedures searches for the server means using the public key to identify the server

means, and the public key identifies a plurality of server computers having different network

addresses as taught by Robertson in order to provide a workable system for allowing a user to

authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

21.     Regarding claim 51, claim 51 is rejected for the same reason as claim 16 as set forth

hereinabove.

22.     Regarding claim 52, Kumar teaches a method for a client computer to find a network

address of a server computer, the method comprising:

        performing a primary search procedure, the primary search procedure including searching

a local storage of the client computer system for the network address of the server computer

(Searching the URL in the memory cache "The process proceeds to block 402 to examine

whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 27-

28);

        performing a backup search procedure if the network address of the server computer is

not found using the primary search procedure DNS lookup as backup search procedure "If the

requested URL host name is not in the cache, the process proceeds from block 402 to block 404,

where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5

lines 34-37) and

        establishing a connection with the server computer using the network address found

(Once detect the most preferred server address and establish to the server "The address listed on

the top of the sorted preferred list is the most preferred server address, which points to the most

preferred server or the optimal site is addressed by the most preferred server address" see

Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly disclose the backup search procedure including searching a

configuration record of the client computer system for the network address of the server

computer.

However Robertson teaches the he backup search procedure including searching a

configuration record of the client computer system for the network address of the server

computer (Software on the user's computer also determines additional public information about

the IP network and then acquires configuration information from the IPSAP central server and

the local IPSAP base server" see Robertson: ¶[0007]) in order to provide a workable system for

allowing a user to authenticated across multiple IP networks and road at will (see Robertson:

¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) the backup search procedure including

searching a configuration record of the client computer system for the network address of the

server computer as taught by Robertson in order to provide a workable system for allowing a

user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

23.     Regarding claim 53, Kumar teaches the method of claim 52 as described hereinabove.

Robertson further teaches the server computer is a password server computer having a public key

that is an identifier of the server computer and the primary search procedure or the backup search

procedure searches for the server computer using the public key to identify the server computer,

said public key identifying a plurality of server computers having different network addresses.

(unique identifier name for the each IPSAP base server "Each IPSAP base server is given a

unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology

(IETF RFC 1991 PGP Message Exchange Formats) to identify … and then returning the IP

addresses of the destination IPSAP based server the PGP public key for the requested IPSAP

base server" see Robertson: ¶[0005]).

24.     Regarding claim 54, Kumar teaches a method for a client computer to find a network

address of a server computer, the method comprising:

        performing a primary search procedure Searching the URL in the memory cache "The

process proceeds to block 402 to examine whether the requested URL host name is in the local

cache memory" see col.5 lines 27-28);

        performing a backup search procedure if the network address of the server computer is

not found using the primary search procedure (DNS lookup as backup search procedure "If the

requested URL host name is not in the cache, the process proceeds from block 402 to block 404,

where the process initiates a DNS lookup for the requested URL host name see col.5 lines 34-

37"), and

        establishing a connection with the server computer using the network address

found (Once detect the most preferred server address and establish to the server "The address

listed on the top of the sorted preferred list is the most preferred server address, which points to

the most preferred server or the optimal site is addressed by the most preferred server address"

see Kumar: col.7 lines 48-56; Fig.4 Step 410).

        Kumar does not explicitly disclose backup search procedure searching an authentication

record for the network address of the server computer.

However Robertson teaches the backup search procedure searching an authentication record for the network address of the server computer (remote authentication the IPSAP base server when allowing building trust relationship between server and client "Remote Authentication Dial In User Service (RADIUS) authentication (IETF RFC 2138) is used to interface the IPSAP base server with the existing authentication program" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the backup search procedure searching an authentication record for the network address of the server computer as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

25.     Regarding claim 65, Kumar teaches a method for a client computer to find a network address of a password server computer having a public key, the method comprising:

searching for a network address of the server computer using a backup search procedure if the address of the server computer cannot be identified using a primary search procedure (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37); and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most

preferred server or the optimal site is addressed by the most preferred server address" see

Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the public key to identify the server computer, and

the public key is shared by a plurality of server computers each respectively having different

network addresses from each other.

However Robertson teaches the public key to identify the server computer, and the public

key is shared by a plurality of server computers each respectively having different network

addresses from each other (unique identifier name for the each IPSAP base server and server

return IP addresses of the destination IPSAP based server and public key and the PGP Public key

for the requested IPSAP base server "Each IPSAP base server is given a unique identifier name

(net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP

Message Exchange Formats) to identify ... and then returning the IP addresses of the destination

IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson:

¶[0005]) in order to provide a workable system for allowing a user to authenticated across

multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) the one or more of said search

procedures searches for the server computer using the public key to identify the server computer,

and the public key identifies a plurality of server computers having different network addresses

as taught by Robertson in order to provide a workable system for allowing a user to authenticated

across multiple IP networks and road at will (see Robertson: ¶[0004]).

26.     Claims 55 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar

et al. (US 6,795,434) in view of Gulko et al. (US 2003/0177240 A1).

27.     Regarding claim 55, Kumar teaches a method for a client computer to find a network

address of a server computer, the method comprising:

performing a primary search procedure (Searching the URL in the memory cache "The

process proceeds to block 402 to examine whether the requested URL host name is in the local

cache memory" see col.5 lines 27-28);

performing a backup search procedure if the network address of the server computer is

not found using the primary search procedure (DNS lookup as backup search procedure "If the

requested URL host name is not in the cache, the process proceeds from block 402 to block 404,

where the process initiates a DNS lookup for the requested URL host name see col.5 lines 34-

37"), and

establishing a connection with the server computer using the network address

found (Once detect the most preferred server address and establish to the server "The address

listed on the top of the sorted preferred list is the most preferred server address, which points to

the most preferred server or the optimal site is addressed by the most preferred server address"

see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the backup search procedure determining whether

the server computer is running on a CPU that is the same CPU on which the client computer is

running in order to determine the network address of the server computer.

However Gulko teaches the backup search procedure determining whether the server

computer is running on a CPU that is the same CPU on which the client computer is running in

order to determine the network address of the server computer (whether the resource on the same

processor by using inter process communication (IPC) "That resource can be the same or another

processor resident on the machine that is executing application 60, or can be another machine

connected via a network 4" see Gulko: ¶[0137]; ¶[0151]) in order to reduction computation time

and increase in result accuracy (see Gulko: ¶[0012]).

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Kumar to include (or to use, etc.) the backup search procedure

determining whether the server computer is running on a CPU that is the same CPU on which the

client computer is running in order to determine the network address of the server computer as

taught by Gulko in order to reduction computation time and increase in result accuracy (see

Gulko: ¶[0012]).

28.     Regarding claim 57, the modified Kumar taught the method of claim 55 as described

hereinabove. Gulko further teaches the step of determining whether the server computer is

running on the same CPU of the client computer comprises sending out an inter process

communication to the CPU (whether the resource on the same processor by using inter process

communication (IPC) "That resource can be the same or another processor resident on the

machine that is executing application 60, or can be another machine connected via a network 4"

see Gulko: ¶[0137]; ¶[0151]).


29.     Claims 56 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar et al.

(US 6,795,434) in view of Gulko et al. (US 2003/0177240 A1) and further in view of Lavian (US

7, 039,724)

30.      Regarding claim 56, the modified Kumar taught the method of claim 55 as described

hereinabove. The modified Kumar does not teaches the step of determining whether the server

computer is running on the same CPU as the client computer comprises using a loop back

address of the server computer.

However Lavian further teaches wherein determining whether the server computer is

running on the same CPU as the client computer comprises: using a loop back address of the

server computer (using the loopback address to test whether the device is local node or not "This

loopback address is a self-referential address which identifies the local network device on the

network without sending packets of information over the actual network" see Lavian: col. 10

lines 44-50) in order to provide alternate way to finding network address for fault tolerant

purpose of Lavian.

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of the modified Kumar to include (or to use, etc.) the public key is an

identifier of the server computer and the public key identifies a plurality of server computers

having different network address as taught by Lavian in order to provide alternate way to finding

network address for fault tolerant purpose of Lavian.


## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action.  Accordingly, **THIS ACTION IS MADE FINAL**.  See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action.  In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action.  In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.


Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Guang Li whose telephone number is (571) 270-1897.  The

examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jeff Pwu can be reached on (571) 272-6798.  The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system.  Status information for published applications

may be obtained from either Private PAIR or Public PAIR.  Status information for unpublished

applications is available through Private PAIR only.  For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

GL
Patent Examiner

/Kenny S Lin/
Primary Examiner, Art Unit 2478